

PATENT ABSTRACTS OF JAPAN

(11)Publication number :

2001-134181

(43)Date of publication of application : 18.05.2001

(51)Int.Cl.

G09C 1/00

(21)Application number : 11-311902

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 02.11.1999

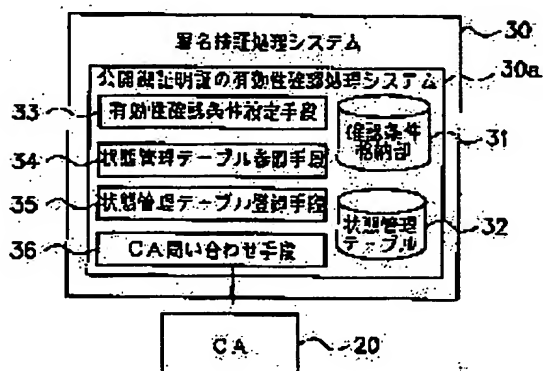
(72)Inventor : HASHIMOTO SHOICHI
NAKAHARA SHINICHI

(54) EFFECTVENESS CONFIRMATION SYSTEM FOR PUBLIC KEY CERTIFICATE AND METHOD THEREFOR AND MEDIUM RECORDED WITH ITS PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a system capable of confirming the effectiveness of a public key certificate corresponding to the request of a signature verifying system by CA access smaller than that in the conventional system while reliability of the system does not depend on the managing policy of a CA, and a method therefor and medium on which its program is recorded.

SOLUTION: When the effectiveness confirming and processing requests of a public key certificate is generated, whether the confirming of the effectiveness satisfying conditions in a confirmation condition storage part 31 is possible or not with respect to the certificate is confirmed from a status management table 32 by a status management table referring means 34 and when the confirming of the effectiveness of the certificate is possible, this system returns status information to the origin of the request and, besides, when it is impossible, the system requests the confirmation to a CA 20 by using a CA inquiry means 36 and the system registers the result of the confirmation and the data and hour when the status is confirmed in the management table 32 by a status management table registering means 35 and also the system returns status information to the origin of the request.



LEGAL STATUS

[Date of request for examination] 30.10.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3466975

(19) 日本国特許庁 (JP)

(12) 特許公報 (B 2)

(11) 特許番号

特許第 3 4 6 6 9 7 5 号

(P 3 4 6 6 9 7 5)

(45) 発行日 平成15年11月17日 (2003. 11. 17)

(24) 登録日 平成15年8月29日 (2003. 8. 29)

(51) Int. Cl. 7

識別記号

F I

H 0 4 L 9/08

H 0 4 L 9/00 6 0 1 B

6 0 1 F

請求項の数 6

(全 8 頁)

(21) 出願番号 特願平11-311902

(22) 出願日 平成11年11月2日 (1999. 11. 2)

(65) 公開番号 特開2001-134181 (P2001-134181A)

(43) 公開日 平成13年5月18日 (2001. 5. 18)

審査請求日 平成13年10月30日 (2001. 10. 30)

(73) 特許権者 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 橋本 正一

東京都千代田区大手町2丁目3番1号 日本
電信電話株式会社内

(72) 発明者 中原 慎一

東京都千代田区大手町2丁目3番1号 日本
電信電話株式会社内

(74) 代理人 100069981

弁理士 吉田 精孝

審査官 中里 裕正

最終頁に続く

(54) 【発明の名称】 公開鍵証明証の有効性確認システム及びその方法並びにそのプログラムを記録した媒体

1

(57) 【特許請求の範囲】

【請求項 1】 CA が管理・発行する証明証であって署名検証に用いる公開鍵証明証が無効化されていないことを確認するための公開鍵証明証の有効性確認システムにおいて、

署名検証に用いる公開鍵証明証の有効性を確認した最新の日時が公開鍵証明証の有効性確認処理要求の発生時からみて何時間以内であれば良いかの条件を格納する確認条件格納部と、

公開鍵証明証の有効性を確認した時の確認結果が有効か無効かの状態情報を状態確認日時とともに格納する状態管理テーブルと、

署名検証に用いる公開鍵証明証の有効化の有無を CA へ確認依頼する CA 問い合わせ手段と、

初期設定時に、前記確認条件格納部に前記確認条件を設

2

定する有効性確認条件設定手段と、

公開鍵証明証の有効性確認処理要求の発生時に、その公開鍵証明証に対し、確認条件格納部に設定された確認条件を満たすか否かを状態管理テーブルの状態確認日時より確認し、確認条件を満たす場合は、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却し、確認条件を満たさない場合は、CA 問い合わせ手段を起動する状態管理テーブル参照手段と、

CA 問い合わせ手段により CA から取得した公開鍵証明証の有効性の確認結果とその状態確認日時を状態管理テーブルへ登録するとともに、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却する状態管理テーブル登録手段とを具備することを特徴とする公開鍵証明証の有効性確認システム。

【請求項 2】 公開鍵証明証の有効性確認処理要求の発

生時から予め設定した所定の時間を差し引いた日時が、状態管理テーブル内の状態確認日時以前であれば確認条件を満たすとすることを特徴とする請求項 1 記載の公開鍵証明証の有効性確認システム。

【請求項 3】 CA が管理・発行する証明証であって署名検証に用いる公開鍵証明証が無効化されていないことを確認するための公開鍵証明証の有効性確認方法において、

署名検証に用いる公開鍵証明証の有効性を確認した最新の日時が公開鍵証明証の有効性確認処理要求の発生時からみて何時間以内であれば良いかの条件を格納する確認条件格納部と、

公開鍵証明証の有効性を確認した時の確認結果が有効か無効かの状態情報を状態確認日時とともに格納する状態管理テーブルとを用い、

初期設定時に、前記確認条件格納部に前記確認条件を設定し、

公開鍵証明証の有効性確認処理要求の発生時に、その公開鍵証明証に対し、確認条件格納部に設定された確認条件を満たすか否かを状態管理テーブルの状態確認日時より確認し、

確認条件を満たす場合は、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却し、

確認条件を満たさない場合は、署名検証に用いる公開鍵証明証の無効化の有無を CA へ確認依頼し、

CA から取得した公開鍵証明証の有効性の確認結果とその状態確認日時を状態管理テーブルへ登録するとともに、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却することを特徴とする公開鍵証明証の有効性確認方法。

【請求項 4】 公開鍵証明証の有効性確認処理要求の発生時から予め設定した所定の時間を差し引いた日時が、状態管理テーブル内の状態確認日時以前であれば確認条件を満たすとすることを特徴とする請求項 3 記載の公開鍵証明証の有効性確認方法。

【請求項 5】 CA が管理・発行する証明証であって署名検証に用いる公開鍵証明証が無効化されていないことを確認するための公開鍵証明証の有効性確認プログラムを記録した媒体において、

前記プログラムはコンピュータに読み取られた際、該コンピュータに、

署名検証に用いる公開鍵証明証の有効性を確認した最新の日時が公開鍵証明証の有効性確認処理要求の発生時からみて何時間以内であれば良いかの条件を格納する確認条件格納部と、

公開鍵証明証の有効性を確認した時の確認結果が有効か無効かの状態情報を状態確認日時とともに格納する状態管理テーブルとを設け、

初期設定時に、前記確認条件格納部に前記確認条件を設定し、

公開鍵証明証の有効性確認処理要求の発生時に、その公開鍵証明証に対し、確認条件格納部に設定された確認条件を満たすか否かを状態管理テーブルの状態確認日時より確認し、

確認条件を満たす場合は、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却し、

確認条件を満たさない場合は、署名検証に用いる公開鍵証明証の無効化の有無を CA へ確認依頼し、

CA から取得した公開鍵証明証の有効性の確認結果とその状態確認日時を状態管理テーブルへ登録するとともに、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却する処理を実行させることを特徴とする公開鍵証明証の有効性確認プログラムを記録した媒体。

【請求項 6】 公開鍵証明証の有効性確認処理要求の発生時から予め設定した所定の時間を差し引いた日時が、状態管理テーブル内の状態確認日時以前であれば確認条件を満たすとすることを特徴とする請求項 5 記載の公開鍵証明証の有効性確認プログラムを記録した媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子署名を検証する際に用いる公開鍵証明証の有効性を確認するためのシステム及びその方法並びにそのプログラムを記録した媒体に関するものである。

【0002】

【従来の技術】公開鍵暗号を用いた電子署名技術により、利用者の本人確認や通信路における改竄の有無の確認を行うシステムでは、認証機関 (Certification Authority: 以下、CA と略す。) が発行する公開鍵証明証を用いて電子署名の検証が行われる。公開鍵証明証には、信頼性を低下させないために利用可能な有効期間が定められているが、公開鍵に対応する秘密鍵の漏洩や所有者の身元情報の変更等の理由により、有効期間内であっても CA が残りの有効期間内の効力を強制的に無効化する場合がある。このため、電子署名を検証する際には、公開鍵証明証が CA によって無効化されていないことを確認して利用する必要がある。

【0003】ここで、署名検証に用いる公開鍵証明証が無効化されていないことを確認する方法としては、CA が定期的に発行する CRL (Certificate Revocation List) と呼ばれる無効化された公開鍵証明証のリストを CA から取得して確認する方法や、CA に公開鍵証明証の状態を直接問い合わせる方法等があった。

【0004】図 1 (a) は CRL を取得して確認する場合のシステム構成を示すもので、署名検証処理システム 10 内の CRL 取得手段 11 により定期的に CA 20 から CRL を取得し、これを記憶部 12 に格納しておき、署名検証が必要となった時に公開鍵証明証有効性確認処理システム 10 a 内の CRL 検索手段 13 により、記憶

10

20

30

40

50

部 1 2 を検索して確認する。この方法では、定期的に C A 2 0 から C R L を取得しているため、署名検証時に C A 2 0 にアクセスすることなく、最も新しく取得した C R L を用いて公開鍵証明証の無効化の有無を確認することになる。

【0005】また、図 1 (b) は C A に直接確認する場合のシステム構成を示すもので、署名検証が必要となった時に公開鍵証明証有効性確認処理システム 1 0 b 内の C A 問い合わせ手段 1 4 により、C A 2 0 に直接問い合わせ確認する。この方法では、C A 2 0 にアクセスした時点における公開鍵証明証の無効化の有無を確認することになる。

【0006】

【発明が解決しようとする課題】前者の C R L を取得して確認するシステムの場合、最新の C R L を取得した以降に無効化された公開鍵証明証の情報は、次の C R L が発行されるまで確認することができないため、署名検証に用いる公開鍵証明証が、最新の C R L を取得した以降の日時において無効化されていないことを確認することができない。従って、この C R L の発行間隔が長いほど、署名検証時における公開鍵証明証の有効性確認処理の信頼性が低下するという課題があった。また、C R L の発行間隔は C A の運営方針によって定められることから、C A の運営方針によってシステムが行う署名検証処理の信頼性が左右されてしまうという課題があった。

【0007】一方、後者の C A に直接確認するシステムの場合、問い合わせた時点における公開鍵証明証の無効化の有無を確認することができるため、システムが C A に対して確認要求を出すことによって、署名検証時における公開鍵証明証の有効性を常に確認することができる反面、その確認の度に C A へのアクセスが生じ、通信コストがかかるという課題があった。

【0008】本発明の目的は、C A の運営方針に信頼性が左右されることなく、かつ従来より少ない C A アクセスによって、署名検証処理システムの要求に応じた公開鍵証明証の有効性を確認し得る公開鍵証明証の有効性確認システム及びその方法並びにそのプログラムを記録した媒体を提供することにある。

【0009】

【課題を解決するための手段】図 2 は本発明のシステム構成を示すもので、図中、2 0 は C A、3 0 は本発明の公開鍵証明証有効性確認処理システム 3 0 a を含む署名検証処理システムであり、公開鍵証明証有効性確認処理システム 3 0 a は、確認条件格納部 3 1、状態管理テーブル 3 2、有効性確認条件設定手段 3 3、状態管理テーブル参照手段 3 4、状態管理テーブル登録手段 3 5 及び C A 問い合わせ手段 3 6 を具備している。以下、これらの各手段の詳細について説明する。

【0010】・確認条件格納部 3 1

システム要求として署名検証に用いる公開鍵証明証の有

効性を少なくともいつの時点まで確認することが必要であるかの条件（確認条件）を格納する記憶領域。

【0011】・状態管理テーブル 3 2

図 3 に示すように、公開鍵証明証（ここではその識別情報）に対応してこれが有効か無効かの状態情報を状態確認日時とともに格納する記憶領域。

【0012】・有効性確認条件設定手段 3 3

システム初期設定時に、前記確認条件格納部 3 1 に前記確認条件を設定する手段。

10 【0013】・状態管理テーブル参照手段 3 4

公開鍵証明証の有効性確認処理要求の発生時に、その公開鍵証明証に対し、確認条件格納部 3 1 に設定された確認条件を満たす有効性の確認が可能か否かを状態管理テーブル 3 2 より確認し、確認可能な場合は、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却し、確認不可能な場合は、C A 問い合わせ手段 3 6 を起動する手段。

【0014】・状態管理テーブル登録手段 3 5

20 C A 問い合わせ手段 3 6 により C A 2 0 から取得した公開鍵証明証の有効性の確認結果とその状態確認日時を状態管理テーブル 3 2 へ登録する（この際、同一の公開鍵証明証識別情報に対する状態情報が既に存在している場合には、その情報を更新する。）とともに、その状態情報を公開鍵証明証の有効性確認処理の要求元に返却する手段。

【0015】・C A 問い合わせ手段 3 6

署名検証に用いる公開鍵証明証の無効化の有無を C A 2 0 へ確認依頼する手段（図 1 の (b) 中の C A 問い合わせ手段 1 4 と同一）。

30 【0016】次に、上記の各構成要素による公開鍵証明証の有効性確認方法の流れを、図 4 を用いて説明する。

【0017】（1）システム初期設定時において、有効性確認条件設定手段 3 3 により、署名検証に用いる公開鍵証明証の有効性を、少なくともいつの時点まで確認することが必要であるかの条件を、確認条件格納部 3 1 に格納する。

【0018】（2）署名検証処理システム 3 0 が署名検証に用いる公開鍵証明証の有効性を確認する必要が発生した際、まず、状態管理テーブル参照手段 3 4 により、その公開鍵証明証に対し、確認条件格納部 3 1 に設定された条件を満たす有効性の確認が既に行われているか（確認可能か否か）を、状態管理テーブル 3 2 より確認する。そして、その条件を満たした有効性が確認されるか、あるいは無効化されていることが確認された場合、その状態情報を状態確認処理の要求元、即ち署名検証処理システム 3 0 に返却して状態確認処理を終了する。また、そのどちらも確認されなかった場合、つまり確認条件外の有効性が確認されるか、あるいはその公開鍵証明証の状態情報が状態管理テーブル 3 2 内に存在しなかった場合には（3）に進む。

【0019】(3) CA問い合わせ手段36を用いて、署名検証に用いる公開鍵証明証の有効性の有無を、CA20へアクセスして確認する。

【0020】(4) 状態管理テーブル登録手段35により、(3)でCA20から取得した公開鍵証明証の有効性確認結果とその状態確認日時を状態管理テーブル32内に登録し、その後、その状態情報を状態確認処理の要求元に返却して確認処理を終了する。

【0021】以上説明したシステム及び処理方法を用いることにより、署名検証に用いる公開鍵証明証の有効性を確認する際、CAに問い合わせた公開鍵証明証の有効性の確認結果を状態管理テーブルに保管し、その情報を以降の公開鍵証明証の有効性確認処理で活用することが可能になる。

【0022】従って、署名検証に用いる公開鍵証明証に対して、状態管理テーブル内の情報を用いて署名検証処理システムの要求条件を満たす有効性が確認可能な場合には、CAへのアクセスが不要となるため、従来よりも少ないCAアクセス回数により、署名検証処理システムの要求に応じた公開鍵証明証の有効性確認が可能となる。

【0023】なお、本発明は、CPU、メモリ、外部記憶装置等のコンピュータシステム（ハードウェア）とともに、図4の流れ図に示される手順を備えたプログラム（ソフトウェア）を記録した媒体によって実現することもできる。

【0024】

【発明の実施の形態】次に、図5、6、7及び8を用いて、本発明の実施の形態を説明する。

【0025】まず、システム初期設定時において、署名検証処理システムが要求する公開鍵証明証の有効性確認条件の設定について、図5を用いて説明する。

【0026】本実施の形態では、システムが署名検証に用いる公開鍵証明証は、少なくともその署名検証時の12時間前までの有効性が確認されていることを、公開鍵証明証の有効性確認処理におけるシステムの要求条件であると仮定する。

【0027】・状態確認条件設定手段33

(a) システム初期設定時において、システムの要求条件である公開鍵証明証の有効性確認条件を設定するため、エディタ機能を用いて、仮定した条件に対応する「(署名検証時の日時) - (12時間) < (状態管理テーブル内の状態確認日時)」の条件式を記述する。この条件式は、状態管理テーブル32内の状態確認日時が、署名検証時の日時の12時間前よりも後の日時を示すことを意味する。エディタ機能は、コンピュータシステムにおいて一般的に利用可能な機能である。

【0028】(b) ファイル入出力機能を用いて、

(a) の確認条件を確認条件格納部31に保管する。フ

ァイル入出力機能は、コンピュータシステムにおいて一般的に利用可能な機能である。

【0029】次に、公開鍵証明証の有効性を確認する際に、状態管理テーブル32で有効性が確認できなかった場合に、CAにアクセスしてその有効性を確認するようすを、図6を用いて説明する。図6の実施の形態では、1999年6月21日15時に、公開鍵証明証の状態確認処理が要求されたと仮定し、また、その時点における状態管理テーブルは、図7の(a)の状態であったと仮定する。

【0030】・状態管理テーブル参照手段34

(a) まず、公開鍵証明証解析機能を用いて、署名検証に用いる公開鍵証明証からその識別情報である発行者名、所有者名、通し番号の情報を取得する。本実施の形態では、発行者名が「CA-1」、所有者名が「利用者A」、通し番号が「1001」である識別情報が取得できたものとする。公開鍵証明証解析機能は、例えば公開鍵証明証の標準形式であるX.509形式の公開鍵証明証の内容を解析する機能が既に実現されており、容易に利用可能である。

【0031】(b) 次に、ファイル入出力機能を用いて、システム初期設定時に格納した確認条件格納部31から有効性確認条件を参照し、この確認条件式の左辺を計算するため、時刻計算機能を用いて署名検証時の日時の12時間前を計算し、「(1999年6月21日15時) - (12時間) = (1999年6月21日3時)」を算出する。時刻計算機能は、時刻を扱うコンピュータシステムにおいて一般的に実現されている機能である。

【0032】(c) 続いて、テーブル参照機能を用いて、(ア) (a) で取得した公開鍵証明証の識別情報（発行者名が「CA-1」、所有者名が「利用者A」、通し番号が「1001」）で、かつ(イ) (b) の計算結果と確認条件式から「1999年6月21日3時 < 状態管理テーブル内の状態確認日時」を満たし、かつ(ウ) 状態情報が「有効」である情報が、状態管理テーブル32内に存在するかを確認する。

【0033】この(ア)～(ウ)の全ての条件に合致する情報が存在した場合、署名検証に用いる公開鍵証明証の有効性が、少なくとも12時間前以内に確認されていることになり、システムが要求する確認条件を満たすことになる。本実施の形態においては、図7の(a)に示されている状態管理テーブルに、(ア)～(ウ)の全ての条件に合致する情報は存在しないため、次の処理に進む。テーブル参照機能は、例えば市販のDBシステム等で実現されているDB参照機能等が利用可能である。

【0034】・CA問い合わせ手段36

(d) (c) で、条件に合致する情報が状態管理テーブル32内に存在しなかったため、CAサービスアクセス機能を用いて、発行者名が「CA-1」、所有者名が「利用者A」、通し番号が「1001」の識別情報を持

10

20

30

40

50

つ公開鍵証明証の無効化の有無についてCAへ確認依頼する。本実施の形態では、CAから状態確認結果として「有効」の情報が返却されたとする。公開鍵証明証の状態を確認するためのCAサービスアクセス機能は、例えば既存のCAが提供する公開鍵証明証検証サービス等を利用することにより実現可能である。

【0035】・状態管理テーブル登録手段35

(e) (d)で確認依頼を行った日時情報とCAから返却された対象公開鍵証明証の有効性確認結果を、テーブル更新機能を用いて、状態管理テーブル32内の発行者名が「CA-1」、所有者名が「利用者A」、通し番号が「1001」の識別情報に対応する状態確認日時情報と状態情報の欄に上書きする。本実施の形態では、CAへの状態確認日時が、1999年6月21日15時00分10秒に完了したと仮定している。図7の(b)に更新後の状態管理テーブル32の状況を示しておく。テーブル更新機能は、例えば市販のDBシステムにおいてDBの情報を書き換えるためのDB更新機能等が利用可能である。

【0036】(f)その後、戻り値返却機能を用いて公開鍵証明証の状態確認処理の要求元に状態情報を返却して確認処理を終了する。戻り値返却機能は、通常のプログラム作成において利用可能な機能である。

【0037】続いて、公開鍵証明証の有効性をCAにアクセスせずに、状態管理テーブルの参照のみで確認可能となる実施の形態について、図8を用いて説明する。図8は、図6の処理の後、再度同一の公開鍵証明証を用いた署名検証処理が行われた場合の実施の形態を示しており、1999年6月21日16時に公開鍵証明証の状態確認処理が開始され、また、この時点における公開鍵証明証の状態管理テーブルは、図7の(b)に示す状態であったとして説明する。

【0038】・状態管理テーブル参照手段34

(a) 公開鍵証明証の状態確認処理の開始(要求)を受けて、図6の時と同様に、公開鍵証明証解析機能を用いて署名検証に用いる公開鍵証明証から識別情報の取得を行い、発行者名が「CA-1」、所有者名が「利用者A」、通し番号が「1001」である識別情報を取得する。

【0039】(b)次に、ファイル入出力機能を用いて、システム初期設定時に格納した確認条件格納部31から有効性確認条件を参照し、この確認条件式の左辺を計算するため、時刻計算機能を用いて、署名検証時の日時の12時間前を計算し、「(1999年6月21日16時) - (12時間) = (1999年6月21日4時)」を算出する。

【0040】(c)続いて、テーブル参照機能を用いて、(ア)(a)で取得した公開鍵証明証の識別情報(発行者名が「CA-1」、所有者名が「利用者A」、通し番号が「1001」)で、かつ(イ)(b)の計算

結果と確認条件式から「1999年6月21日4時<状態管理テーブル内の状態確認日時」を満たし、かつ、

(ウ)状態情報が「有効」である情報が、状態管理テーブル内に存在するかを確認する。図7の(b)より、ハッチング部分の情報が上記(ア)～(ウ)の全ての条件に合致する情報であるため、戻り値返却機能を用いて公開鍵証明証の状態確認処理の要求元に状態情報である「有効」を返却して確認処理を終了する。

【0041】上記のように、署名検証処理システムが署名検証に用いる公開鍵証明証の有効性を確認する際、その公開鍵証明証が、予め定めた署名検証に用いるための有効性確認条件に合致するかの確認を、状態管理テーブル内に登録されている、過去にCAに問い合わせた有効性確認結果から判断可能な場合には、CAへのアクセスが不要となるため、従来よりも少ないCAアクセス回数により、システムの要求に応じた公開鍵証明証の有効性確認が可能となる。

【0042】

【発明の効果】以上説明したように、本発明によれば、署名検証に用いる公開鍵証明証の有効性の確認において、過去にCAに問い合わせた有効性確認結果を、以降の有効性確認処理に活用することが可能となり、活用できた場合にはCAへのアクセスが不要となるため、短期間で同一利用者の電子署名を複数回検証する必要があるシステム等では、CAアクセスのために費やされていた通信コストが削減され、署名検証処理の処理性能を向上させることが可能となる。また、1時間前、あるいは1日前等というように、署名検証時から遡っていつの時点までにおける公開鍵証明証の有効性が確認されれば良いかという条件をシステム自身が任意に設定することが可能であるため、システムの要求に応じて公開鍵証明証の有効性確認処理の正確さを制御することが可能となる。

【図面の簡単な説明】

【図1】従来の公開鍵証明証の有効性確認システムの構成図

【図2】本発明の公開鍵証明証の有効性確認システムの構成図

【図3】公開鍵証明証の状態情報を保管する状態管理テーブルの構成図

【図4】本発明の公開鍵証明証の有効性確認方法の処理の流れをシステムの構成要素とともに示す図

【図5】システムの要求に基づく有効性確認条件の設定の実施の形態を示す図

【図6】状態管理テーブルでは公開鍵証明証の有効性が確認できず、CAにアクセスして確認する実施の形態の説明図

【図7】実施の形態における状態管理テーブルの内容の一例を示す図

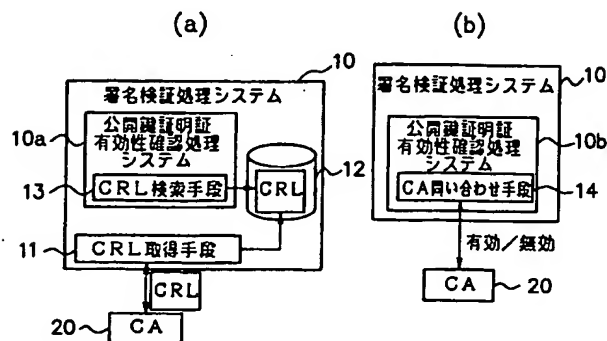
【図8】CAにアクセスせず、状態管理テーブルの参照のみで公開鍵証明証の有効性を確認可能な実施の形態の

説明図

【符号の説明】

20 : CA、30 : 署名検証処理システム、30a : 公開鍵証明書有効性確認処理システム、31 : 確認条件格納部

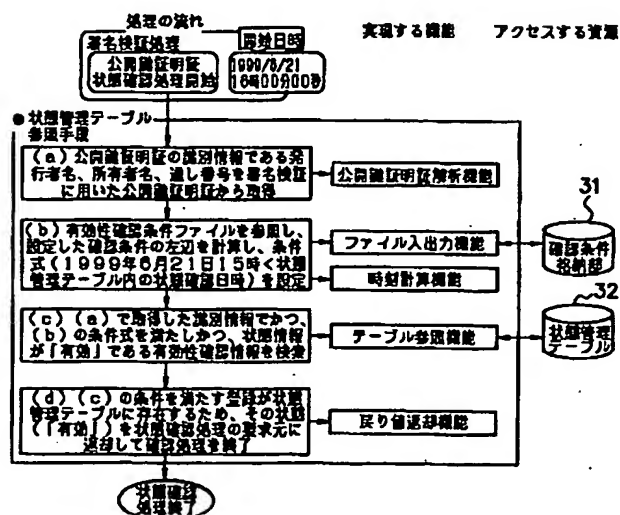
【図1】



【図3】

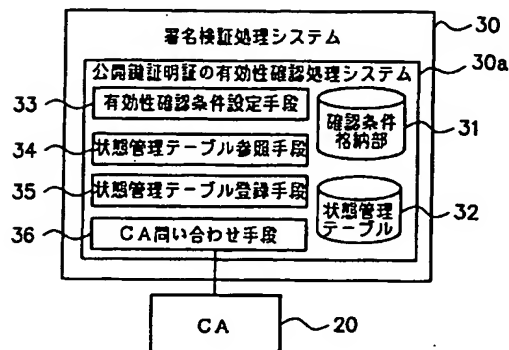
公開鍵証明書識別情報	状態確認日時	状態
公開鍵証明書1	1999/06/20 10時20分00秒	有効
公開鍵証明書2	1999/06/20 13時00分00秒	有効
公開鍵証明書3	1999/06/21 10時00分00秒	無効

【図8】

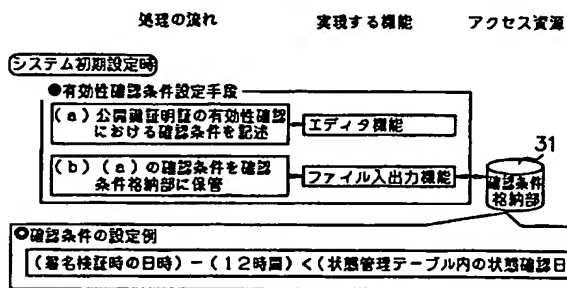


納部、32 : 状態管理テーブル、33 : 有効性確認条件設定手段、34 : 状態管理テーブル参照手段、35 : 状態管理テーブル登録手段、36 : CA問い合わせ手段。

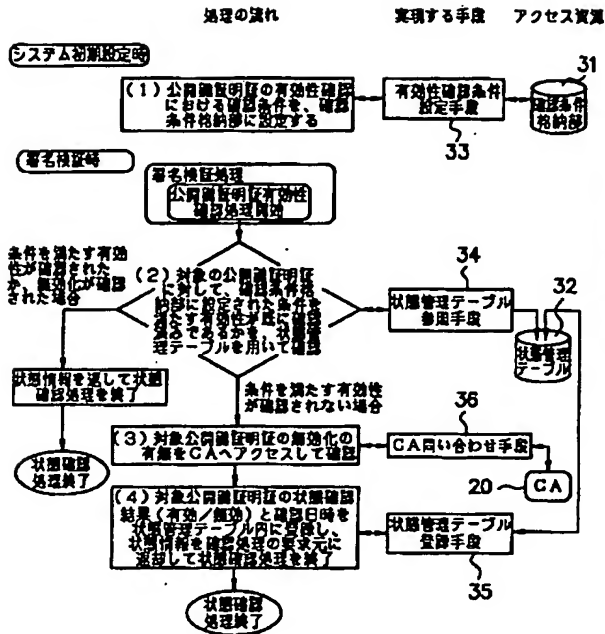
【図2】



【図5】

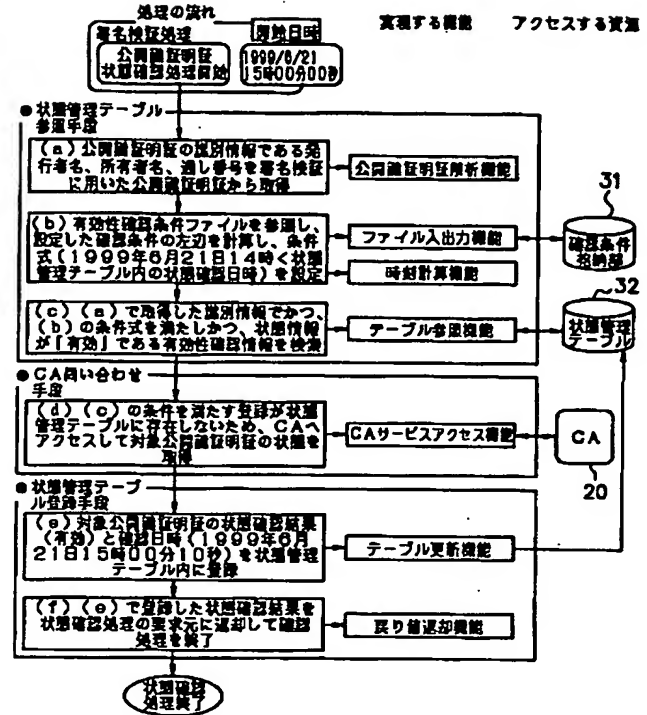


【図 4】



【図 7】

【図 6】



(a) 公開鍵証明書の有効性確認処理前の状態

公開鍵証明書の識別情報			状態確認日時	状態
発行者名	所有者名	シリアル番号		
CA-1	利用者A	1001	1999/06/20 10時00分00秒	有効
CA-1	利用者B	1005	1999/06/20 13時00分00秒	有効
CA-2	利用者C	2001	1999/06/21 10時00分00秒	有効

(b) 公開鍵証明書の有効性確認処理後の状態

公開鍵証明書の識別情報			状態確認日時	状態
発行者名	所有者名	シリアル番号		
CA-1	利用者A	1001	1999/06/21 15時00分10秒	有効
CA-1	利用者B	1005	1999/06/20 13時00分00秒	有効
CA-2	利用者C	2001	1999/06/21 10時00分00秒	有効

フロントページの続き

(56) 参考文献 Can We Eliminate
Certificate Revoca
tion Lists?, Lecture
Notes in Computer
Science, Vol. 1465, p.
178-183

公証システムにおける個人認証方式の
一考察, 1998年電子情報通信学会総合大
会講演論文集, 1998年 3月26日, 基
礎・境界, p. 256

(58) 調査した分野(Int. Cl.⁷, DB名)

H04L 9/08

J I C S T ファイル (J O I S)